REMARKS:

This paper is herewith filed in response to the Examiner's Office Action mailed on May 4, 2009 for the above-captioned U.S. Patent Application. This office action is a rejection of claims 1-30 and 34-37 of the application.

More specifically, the Examiner has rejected claims 1-2, 4-15, 17-24, 26-30, 34-35, and 37 under 35 USC 102(e) as anticipated by Ma (20050021940); and rejected claims 3, 16, 25, and 36 under 35 USC 103(a) as being unpatentable over Ma in view of Ben-David (US20040043790). The Applicants respectfully traverses the rejections.

Claims 1-15, 17-24, 26-27, 29-30, 34-35, and 37 have been amended for clarification. Support for the amendments and new claims can be found at least in paragraphs [0032] to [0045] and [0051] to [0054]. No new matter is added.

With regards to the rejections of independent claims 1 and 12 the applicants note that the exemplary embodiments of the invention relate to at least a method and apparatus to allow devices to establish communication between devices in a radio communications network for access to required services.

The exemplary embodiments of the invention provide that a user of an apparatus, such as an apparatus that is receiving (as in claim 1) or sending (as in claim 12) a request to/from another apparatus for secure communications and exchanging required services, will not be required to enter a shared secret for the secure communication and the required services. According to the exemplary embodiments of the invention, determinations are made, at either (or both) of the receiving apparatus or the sending apparatus as to whether the apparatus is in an operational mode where the user of the apparatus does not wish to be interrupted, and whether a requested required service is associated with a shared secret stored in a memory of the apparatus. Further, if it is determined that the apparatus is in an operational mode where the user of the apparatus does not wish to be interrupted and that a required service is associated with a secret stored in the

memory of the apparatus, then, according to the exemplary embodiments of the invention, the stored shared secret is automatically accessed from the memory of the apparatus without contemporaneous user input (see paragraphs [0030] to [0035] and [0039] to [0044] of the published application). In addition, according to exemplary embodiments of the invention determined operational mode comprises a gaming mode, and the required service comprises a gaming service (see paragraphs [0038] and [0047] of the published application).

The Applicants respectfully submit that the pending claims are patentably distinguishable from the references cited, and the claims should be allowed.

Regarding the rejection of claim 1 the Applicants note that claim 1 has been amended to recite:

> A method, comprising: generating by a first apparatus which controls access to a radio communications network a shared secret at the first apparatus and storing the shared secret in a memory of the first apparatus, wherein the stored secret is associated with an operational mode of the first apparatus; making the stored shared secret available at a second apparatus; receiving a signal from the second apparatus to establish communication with the first apparatus on the radio communications network, where the signal comprises a request for a required service from the first apparatus; determining whether the first apparatus is in the operational mode where a user of the first apparatus does not want to be interrupted and whether the required service is associated with the stored shared secret; and based on the determining, creating a secret key for use in pairing to secure communication between them, where the secret key is created using an algorithm.

The Applicants note that Ma discloses a method wherein a first wireless device may request one or more authentication keys or algorithms in order to respond to a request made by a carrier. According to Ma the first wireless communication device 104 receives a random number from the carrier cell site and the first wireless communication device 104 relays that number to the second wireless communication device 108 (paragraphs [0024], [0029], and [0037]). The second wireless communication device, of Ma, then processes the random number using a subscriber identity module implemented within the second wireless device (par. [0025]). Then, after processing is done, the processed algorithmic output of the subscriber identity module is

transported back to the cell site 120, apparently via the first communication device, where it is evaluated. Ma indicates that if the algorithmic output matches what is calculated at the carrier's site, then there is a successful authentication, (paragraphs [0024], [0029], and [0037]).

The Applicants submit that Ma does not make a determination of the operational mode of the communications device and a determination of whether a required service is associated with a secret stored in the communications device.

The Applicants contend that in all of Ma can not be found anything to disclose or suggest at least where claim 1 recites in part:

> "determining whether the first apparatus is in the operational mode where a user of the first apparatus does not want to be interrupted and whether the required service is associated with the stored shared secret"

Further, the Applicants contend that, for at least the reasons already stated, Ma can not be seen to disclose or suggest at least where claim 1 recites in part:

> "based on the determining, creating a secret key for use in pairing to secure communication between them, where the secret key is created using an algorithm"

The Applicants submit that, for at least this reason, the rejection of claim 1 is improper and the rejection should be removed.

Regarding where the Examiner cites Ben-David in the rejections, the Applicants note that Ben-David, as cited, relates to a handheld device, such as a PDA, that can play videos or run games that are uploaded to it or stored on a memory card inserted into the device (par. [0102]). According to Ben-David, a facilitator and management circuitry communicate with another device, such as a server, to exchange information regarding games with a server. These communications appear to be performed over a phone link or via infra-red communication (paragraphs [0169] and [0189]). The Applicants submit that there can not be found anything in

Ben-David which can be seen to cure the above referenced shortfalls of Ma.

Although the Applicants do not agree that a combination of Ma and Ben-David is even proper, the Applicants submit that, for at least the reasons stated, the proposed combination of Ma and Ben-David would still fail to disclose or suggest claim 1. Thus, the rejection of claim 1 is seen to be improper and the rejection should be removed.

In addition, for at least the reason that independent claims 12, 14, and 34-35 recite features similar to claim 1, as stated above, the references cited can not be seen to disclose or suggest these claims and the rejections should be removed.

In addition, the Applicants submit that the references cited can not be seen to disclose or suggest at least where claim 2 recites in part:

> "for the case it is determined that the first apparatus is in the operational mode where the user of the first apparatus does not want to be interrupted and that the required service is associated with the stored shared secret, then automatically accessing the stored shared secret associated with the required service without contemporaneous user input, or else prompting the user of the first apparatus to enter a shared secret associated with the requested service"

The Applicants respectfully request that the Examiner reconsider and remove the rejection of claim 2.

In addition, for at least the reason that claims 13, 15, 29, and 37 recite features similar to claim 2, as stated above, the references cited are not seen to disclose or suggest these claims and the rejections of these claims should be removed.

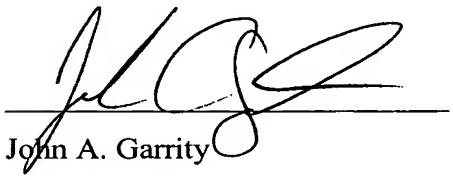
Further, for at least the reason that claims 2-11, claim 13, claims 15-28 and 30, claim 37, and claims 29 and 36 depend from independent claims 1, 12, 14, 34, and 35, respectively, the references cited can not be seen to disclose or suggest these claims.

Further, the Applicants submit that, although not all the rejections are argued against in this Response, the Applicants do not acquiesce to any of the rejections.

Based on the above explanations and arguments, it is clear that the references cited cannot be seen to disclose or suggest claims 1-30 and 34-37. The Examiner is respectfully requested to reconsider and remove the rejections of claims 1-30 and 34-35 and to allow all of the pending claims 1-30 and 34-37 as now presented for examination.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record. Should any unresolved issue remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted:



8/20/09

John A. Garrity
Reg. No.: 60,470
Customer No.: 29683
HARRINGTON & SMITH, PC
4 Research Drive
Shelton, CT 06484-6212
Telephone: (203)925-9400
Facsimile: (203)944-0245
email: jgarrity@hspatent.com

Date

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

8.20.2009
Date

Name of Person Making Deposit